STATEMENT OF

FINANCIAL SERVICES COORDINATING COUNCIL

American Bankers Association
American Council of Life Insurers
American Insurance Association
Securities Industry Association

BEFORE THE SUBCOMMITTEE ON COMMERCE, TRADE AND CONSUMER PROTECTION

COMMITTEE ON ENERGY AND COMMERCE

U.S. HOUSE OF REPRESENTATIVES

May 11, 2006

Statement of the Financial Services Coordinating Council

I am Oliver Ireland with Morrison & Foerster LLP testifying on behalf of the Financial Services Coordinating Council ("FSCC"), whose members are the American Bankers Association, American Council of Life Insurers, American Insurance Association, and Securities Industry Association. The FSCC represents the largest and most diverse group of financial institutions in the United States, consisting of thousands of large and small banks, insurance companies, investment companies, and securities firms. Together, these financial institutions provide financial services to virtually every household in the United States.

The FSCC very much appreciates the opportunity to submit this statement to the Subcommittee concerning the use and misuse of Social Security numbers ("SSNs"). Our comments focus on the integral role of SSNs in United States commerce; the many consumer benefits that result from the use of SSNs by financial institutions; and the potentially negative effects that could occur if undue restrictions are imposed on such use. While the FSCC recognizes that there have been misuses of SSNs, we strongly urge that any legislation intended to address this problem be carefully targeted to specifically identified abuses, such as measures to stop identity theft. We believe it is imperative to avoid restrictions on legitimate and beneficial uses of SSNs.

Our testimony today focuses on three fundamental points:

- ***First***, following the lead of the U.S. Government for the last 65 years, businesses have legitimately used the SSN as a unique identifier of individuals, and this use is now woven into the fabric of consumer and commercial transactions throughout the country. Moreover, this legitimate use of SSNs has produced real benefits for American consumers and taxpayers, and has become critically important for a wide range of government agencies, financial institutions, hospitals, blood banks, and many

other businesses, both large and small.

- ***Second***, broad restrictions on the use of SSNs could have serious unintended consequences, including: higher credit costs; increased fraud and identity theft; fundamental and costly changes to internal business operating systems; decreased consumer service; and costly delays in consumer and commercial transactions. Further restrictions on the use of SSNs may also impede law enforcement purposes, including with respect to money laundering and terrorist financing.

- ***Third***, Congress has enacted privacy and information security protections under the Gramm-Leach-Bliley Act ("GLBA") that, among other things, subject financial institutions to an affirmative and continuing obligation to protect the security and confidentiality of their customer's nonpublic personal information, including SSNs, and establish stringent requirements for financial institutions concerning the use, transfer and protection of SSNs. In addition, more than 20 states have adopted statutes designed to protect the confidentiality of SSNs. Further, state security breach notification laws in some 30 states provide additional incentives to protect SSNs. Moreover, this Committee and other Committees of Congress recently have passed express requirements that would protect the security of SSNs. In light of these current and proposed protections, the FSCC strongly believes that further legislative restrictions on the use and transfer of SSNs by financial institutions are unnecessary.

Our statement also discusses the potentially negative impact of SSN restrictions on the legitimate use by financial institutions of public records.

As the Subcommittee is aware, Congress adopted privacy protections as part of the GLBA. The GLBA subjects the financial services industry to a comprehensive privacy framework that requires the annual disclosure of a financial institution's privacy policies, allows customers to direct the institution not to share their "nonpublic personal information" with nonaffiliated third parties, contains significant prohibitions on the disclosure of detailed account information, and establishes regulatory standards to protect the security of "nonpublic personal information." *Importantly, under the GLBA, SSNs are considered "nonpublic personal information," and thus are already subject to*

significant restrictions on the transfer of, and the ability of others to reuse, such information. Moreover, in 2003, Congress enacted additional legislation addressing concerns over identity theft, as part of its passage of the "Fair and Accurate Credit Transactions Act of 2003." These two Congressional initiatives go straight to the heart of Congressional concerns over identity theft and the efforts of financial institutions to combat this growing problem. In addition, the Committee on Energy and Commerce and other Committees of Congress recently have passed express requirements that would protect the security of SSNs.

As a practical matter, we do not believe that the financial services industry is the subject of the concern that Congressional legislation would attempt to address. We use SSNs, as well as other personal financial information, to assist us in making sound credit decisions, underwriting applications for insurance coverage and performing other ordinary insurance business functions, combating fraud, rooting out identity theft, and uncovering financial support for terrorism. We do not make SSNs accessible to the general public. As a result, we believe that any legislation should be targeted at those entities at the heart of the problem, be they unregulated information brokers, those engaged in illegal pretext-calling, or the like.

Integral Role of Social Security Numbers in U.S. Commercial Activities

To assist the Subcommittee in its deliberations, it may be helpful to review the important role that SSNs play in U.S. commercial activities.

As the Government Accountability Office (GAO) noted in a February 1999 report,[1] the Social Security Administration created the SSN in 1935 as a means to maintain individual earnings records for the purposes of that program. But, Congress soon realized the tremendous value to society of a unique identifier that is common to nearly every American. As a result, it began to require federal government use of the SSN as a common unique identifier for a broad range of wholly unrelated purposes and programs. For example, "a number of federal laws and regulations require the use of the SSN as an individual's identifier to facilitate automated exchanges that help administrators enforce compliance with federal laws, determine eligibility for benefits, or both."[2] These include federal laws applicable to tax reporting, food stamps, Medicaid, Supplemental Security Income, and Child Support Enforcement, among others. Moreover, as the GAO acknowledged, it has repeatedly recommended in numerous reports that the federal government use SSNs as a unique identifier to reduce fraud and abuse in federal benefits programs.[3]

Following the federal government's lead, American businesses complied with federal requirements to use SSNs as identifiers for federal laws unrelated to Social Security, such as income tax reporting. In doing so, they also realized the powerful consumer benefits to be derived from comparable business use of SSNs as a common unique identifier. Thus, businesses began to use SSNs in a manner similar to the federal government, *e.g.,* to match records with other organizations to carry out data exchanges for such legitimate business purposes as transferring and locating assets, tracking patient

[1] "Social Security – Government and Commercial Use of the Social Security Number is Widespread," February 1999, GAO/HEHS-99-28.
[2] *Id.* at 4.
[3] *Id.*

care among multiple health care providers, and preventing fraud and identity theft. Many businesses also use SSNs as an efficient unique identifier for such internal activities as identifying income tax filers.

Similarly, the financial services industry has used the SSN for many decades for a broad range of responsible purposes that benefit consumers and the economy. For example, our nation's remarkably efficient credit reporting system—which has helped make America's affordable and accessible credit the envy of the world—relies fundamentally on the SSN as a common identifier to compile disparate information from many different sources into a single, reliable credit file for a given consumer. Indeed, the banking, insurance, and securities industries each use SSNs for a variety of important regulatory and business transactions. Set forth below is an illustrative sample of the many financial institution uses of SSNs:

- To combat fraud and identity theft;
- To accurately assess underwriting risk;
- To assist in internal benefits tracking;
- To identify and report money laundering and terrorist financing activities;
- To comply with reporting requirements of federal and state tax and securities laws;
- To transfer assets and accounts to third parties;
- To comply with "deadbeat spouse" laws;
- To verify appropriate Department of Motor Vehicle records when underwriting auto insurance;
- To obtain medical information used in underwriting life, disability income, and long-term care insurance polices;
- To locate missing beneficiaries to pay insurance proceeds;

- To locate insurance policies for owners that have lost their policy numbers; and
- To facilitate a multitude of administrative functions.

As noted in the GAO report discussed above, "the uniqueness and broad applicability of the SSN have made it the identifier of choice for government agencies and private businesses, both for compliance with federal requirements and for the agencies' and businesses' own purposes."[4] As a result, the use of SSNs as common unique identifiers has become woven into the very fabric of both government and commercial transactions in this country, and has been so for decades.

In short, the federal government began the use of SSNs for unrelated identification purposes; it required businesses to do the same under certain federal laws; and its use served as an example for businesses, including financial institutions, for over half a century. These uses have produced tremendous efficiencies and benefits for all Americans. The FSCC strongly urges members of Congress to keep such legitimate uses and benefits in the forefront when considering proposals to restrict the use of SSNs.

Unintended Consequences of Broad Restrictions on the Use of Social Security Numbers

As a result of the widespread use of SSNs for legitimate purposes, the FSCC is concerned about the potential unintended consequences of any legislation that is intended to restrict SSN abuses. If legislation is not carefully targeted to avoid these unintended consequences, consumers and the smooth operation of the U.S. economy could be seriously harmed. The following provides some specific examples of such harm:

- **Potential Harm to Consumers.** The use of SSNs allows financial institutions to provide a level of service to customers that would otherwise not be possible. By using these numbers to verify individual identities, credit bureaus and others can quickly provide financial institutions with accurate credit histories and verification information on people seeking credit, insurance, securities, and other financial products. In turn, a financial institution can act swiftly and efficiently on applications or requests related to these products. Use of SSNs also enables financial institutions to provide more seamless administrative service, including, for example, by allowing a life insurer to more easily verify the identity of an individual calling into a call center to change a beneficiary or premium mode or to make some other change to an insurance policy. The FSCC's concern is that a broad restriction on the sale or use of SSNs, however well-intended, could seriously impede the delivery of such important services by driving up processing costs and impairing decision-making.

- **Increased Risk of Fraud and Identity Theft.** SSNs are critical for fraud detection. Banks, insurance companies, and securities firms rely on information available from both public and private sources—with embedded SSNs to ensure correct identification—to check for "inconsistencies" that may suggest the occurrence of fraud or identity theft. The use of these numbers also helps financial institutions verify credit and other information necessary to make sound underwriting decisions that minimize losses. The sophisticated processes used for these purposes rely fundamentally on SSNs as the common unique identifier to assemble accurate and verifiable information for a given individual. That is, without a unique common identifier such as a SSN, we believe it would be *easier*, not harder, for an individual's identity to be stolen. Thus, to reiterate, we believe that Congress should exercise great caution in restricting the use of SSNs so as not to risk an increase in consumer fraud or identity theft—a result that would be squarely at odds with the intended purpose of such restrictions.[5]

- **Market Disruption.** A prohibition on the sale of SSNs could be construed to restrict such activities as the sale of assets among financial institutions. This is so because financial institution assets (*e.g.*, mortgage servicing accounts, credit card accounts, and traditional bank accounts) often use SSNs as the basis for account identification. Also, SSNs are part of policy files that may be transferred by an insurer in connection with a merger or acquisition or as part of a reinsurance agreement. When it sells such an asset or transfers such files, a financial institution could be viewed as technically "selling" the embedded SSN as well. Thus, legislative efforts that "directly or indirectly"

---

[4] *Id*. at 2.

[5] Existing law already includes provisions that prohibit identity theft. For example, stealing someone's identity is punishable by civil and criminal penalties. *See, e.g.,* 18 U.S.C. § 1028. Moreover, the GLBA bans pretext calling—a tool of identity thieves.

limit the transfer, sale, or purchase of SSNs could effectively preclude such plainly legitimate transactions. To address this problem, businesses would need to rework their internal systems completely to eliminate the reliance on such numbers—a massive and needless expense. Accordingly, we believe that any legislative proposal must be crafted to avoid such a significant, unintended consequence.

- **Money Laundering and Terrorist Financing.** Rules implementing section 326 of the USA PATRIOT Act require many financial institutions to obtain a taxpayer identification number, typically a SSN, before opening an account for the individual. The financial institution also must verify the identity of the individual. The verification process is facilitated by the use of SSNs. The section 326 requirement was adopted as part of comprehensive legislation to address terrorism following September 11, 2001. Any limitations on the use of SSNs would need to accommodate the section 326 information collection and verification processes.

Current Protections for Social Security Numbers

The FSCC believes there is no need to further restrict the use of SSNs by *financial institutions* in light of the strong SSN restrictions that apply to such institutions under the GLBA and other laws. The GLBA and its implementing regulations treat a financial institution customer's SSN as protected "nonpublic personal information."[6] As a result, each financial institution is subject to an affirmative and continuing obligation to protect the security of its customers' SSNs, and each customer has the right to block a financial institution from selling or transferring his or her SSN to a nonaffiliated third party or the general public.

There are exceptions to this general rule for legitimate transfers of SSNs, such as ones that are necessary: to carry out a transaction requested by the consumer; to protect against fraud; and to provide necessary identifying information to credit bureaus. *However, even with respect to such legitimate transfers of SSNs, the consumer remains*

[6] *See, e.g.,* 12 C.F.R. § 40.3(o). The regulation generally defines protected "personally identifiable financial information" to include "any information . . . [t]he bank . . . obtains about a consumer in connection with providing a financial product or service to that consumers." *Id*. (emphasis added).

protected because the recipient of the number is prohibited by law from re-using or re-disclosing the number—it may do so only as necessary to carry out the purpose of the exception under which the number was received from the financial institution. Further, the GLBA also requires financial institutions to establish appropriate safeguards to ensure the security of, and to protect against unauthorized access to or use of, SSNs.

In addition, more than 20 states have adopted statutes designed to protect the confidentiality of SSNs. For example, several states have enacted laws that prohibit specified uses of SSNs, including, for example, prohibiting the public display of a SSN. In addition, several states have enacted laws that limit the use of SSNs by state departments and agencies. Further, 30 states have enacted security breach notification laws. These laws generally require a business to notify consumers when a security breach occurs involving sensitive personal information relating to those consumers, including SSNs. Moreover, the Committee on Energy and Commerce and other Committees of Congress recently have passed express requirements that would protect the security of SSNs.

The existing and proposed federal and state protections for SSNs create strong incentives for financial institutions to protect the SSNs that they maintain. In light of these existing and proposed protections, and the corresponding incentives of financial institutions, the FSCC strongly believes that further legislative restrictions on the use and transfer of SSNs by financial institutions are unnecessary.

Concerns Over Restrictions On Access to Public Records

Finally, some concerns have also been expressed regarding the inappropriate use of SSNs available in the public record. The FSCC believes it is

important to remember that a wide range of private sector enterprises—including banks, insurance companies, and securities firms—rely on these records to conduct a broad range of legitimate business activities. For example, financial institutions use public records to:

- Uncover fraud and identity theft;
- Make sound credit and other financial product determinations;
- Verify identities of the customer at the account opening phase;
- Assist in internal security operations (*e.g.*, employee background checks); and
- Otherwise verify identities in order to conduct a broad range of business transactions.

Business reliance upon public records facilitates the efficient operation of the financial and credit markets, limits mistakes, and ensures that consumers receive prompt and lower-cost service. It also helps protect the customer from fraud.

More specifically, to achieve the purposes described above, financial institutions directly use: public records involving liens on real estate; criminal records and fraud detection databases; and similar types of public records. Financial institutions also indirectly use these records for the same purposes by relying on databases developed by third parties that themselves rely on information from public records. Importantly, SSN identifiers are central to ensuring that the information included in these records matches the correct individual. This allows banks, for example, to verify the identity of a person so that a direction from a customer to transfer funds to a third party can be executed without mistake, as well as to check important credit-related characteristics of loan applicants (such as pending bankruptcies, tax liens, or other credit problems).

Moreover, financial institutions employ sophisticated programs that cross-check public information against information supplied by an applicant in order to uncover fraud. For example, if the age information provided by an applicant posing as another individual were inconsistent with other information known about that individual from public records made available through SSN identification, a "red flag" would be raised, which would trigger further checking to uncover the identity theft.

Thus, overly-broad limits on access to public record information would compromise a financial institution's ability to make sound business decisions and to protect its customers. Such limits could also greatly slow the decision-making process of U.S. businesses, to the detriment of consumers and the economy. For example, if a SSN were stricken from a public record, it is possible that the ability to use that record for legitimate purposes would become impractical because of the expense involved in verifying the identity of the person covered by that record. The consequences could include delayed loan approvals, increased consumer costs for products and services, and limits on an institution's ability to discover identity theft on a timely basis.

Even if public entities could still retain SSNs in their internal nonpublic files and financial institutions could obtain access to such files, the cost and delays in efficiently accessing such files would be significant. Ultimately, the cost efficiencies and speed of delivery inherent in our current market system would be compromised. The effect could be the same as denying financial institutions access to such records.

Conclusion

The benefits to society from the legitimate and responsible use of SSNs are real and substantial. As a result, the FSCC believes that policymakers should look

carefully at the unintended consequences that could occur with any proposal that would restrict the use of these numbers. And, because of the existing restrictions on financial institution disclosure of SSNs, including the GLBA, we believe that no new SSN restrictions are required for the financial services industry.
